UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA, Plaintiff, v. MARCUS A. OWENS, Defendant.	Case No. 16-CR-38-JPS **ORDER**

On March 1, 2016, a grand jury sitting in the Eastern District of Wisconsin returned a two-count indictment against Marcus A. Owens. Indictment (Docket #9). Mr. Owens is charged with one count of knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5). (Docket #9). This matter comes before the Court on Mr. Owens's motion to suppress based on the evidence. (Docket #37).

On October 4, 2016, Magistrate Judge David E. Jones issued a Report and Recommendation ("the Report") with this Court, recommending that the motion to suppress be denied. (Docket #62). On October 18, 2016, Mr. Owens filed written objections to the findings pursuant to 28 U.S.C. § 636(b(1)(C). (Docket #65). On October 31, 2016, the government filed a response to the objections, (Docket #74), and on November 7, 2016, Mr. Owens filed a reply (Docket #80). The objections to the Report are now fully briefed and ready for disposition. As discussed below, the Court adopts the recommendation of Magistrate Jones in full and will therefore deny Mr. Owens's motion to suppress the evidence.

1. BACKGROUND

This case arises out a large-scale FBI investigation into a child pornography website. For the purposes of this Order, the Court presumes the parties' familiarity with the background of this case. As discussed in detail below, numerous district courts around the country have already considered nearly the identical issues arising out of the investigation and warrants issued in this case.

In September 2014, FBI agents began investigating a website that appeared to be dedicated to the advertisement and distribution of child pornography. (Affidavit in Support of Application for NIT Warrant ("NIT Warrant Aff.") ¶ 11, Docket #39-2 at 5-37. The website, "Playpen"—referred to in the warrant applications as "Target Website" and "Website A" respectively—had more than 150,000 registered users and contained tens of thousands of posts related to child pornography. (NIT Warrant Aff. ¶¶ 10-13).

Playpen did not reside on the traditional or "open" internet. (NIT Warrant Aff. ¶ 10). Instead, Playpen operated only on the "Tor" network, an open-source software tool which routes communications through multiple computers called "nodes" in order to mask a user's IP address. Users have to download specific Tor software or utilize a Tor "gateway" to get onto the Tor network and then navigate to a site like Playpen. (NIT Warrant Aff. ¶ 7). This process is used to keep the website user's identity anonymous. (NIT Warrant Aff. ¶¶ 7-9).

1.1 The Network Investigative Technique Warrant

In February 2015, the FBI apprehended the administrator of Playpen and took control of the website. (NIT Warrant Aff. ¶ 30). Rather than shut

down Playpen, however, the FBI operated the website from a government facility in the Eastern District of Virginia for close to two weeks in an effort to identify website users. On February 20, 2015, an FBI special agent applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use a Network Investigative Technique ("NIT") to investigate Playpen's users and administrators. In support of the warrant application, the agent submitted a thirty-three-page affidavit that set forth his basis for probable cause to believe that deploying the NIT would uncover evidence and instrumentalities of certain child exploitation crimes. *(See generally* NIT Warrant Aff.).

The NIT involved additional computer instructions that would be downloaded to a user's computer—referred to as an activating computer—along with the site's normal content. (NIT Warrant Aff. ¶ 33). After downloading the additional instructions, the activating computer would transmit certain information to the government-controlled computer located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address. (NIT Warrant Aff. ¶¶ 33-34, 36). The NIT would be deployed each time a user logged onto the government-controlled website. (NIT Warrant Aff. ¶ 36).

On February 20, 2015, United States Magistrate Judge Theresa Carroll Buchanan, sitting in the Eastern District of Virginia, signed the NIT Warrant. (NIT Warrant, Docket #39-2 at 2-4). The face of the NIT Warrant authorized

the government to search property located in the Eastern District of Virginia. (NIT Warrant at 2). Additionally, the NIT Warrant further described the property to be searched in "Attachment A" to the warrant. (NIT Warrant at 2).

Attachment A of the NIT Warrant stated that the warrant "authorize[d] the use of [an NIT] to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." (NIT Warrant at 3). It explained that the computer server, which was located at a government facility in the Eastern District of Virginia, was operating a Tor network child pornography website. Further, it stated that the activating computers were those of any user or administrator who logged into the child pornography website. (NIT Warrant, Docket #39-2 at 3).

Attachment B identified the property to be seized. It listed seven pieces of information to be seized "[f]rom any 'activating' computer": (1) the IP address, and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT; (3) the type of operating system running on the computer; (4) information about whether the NIT had already been delivered to the activating computer; (5) the activating computer's Host Name; (6) the activating computer's active operating system username; and (7) the activating computer's media access control address. (NIT Warrant at 4).

Through the use of the NIT and additional investigation, FBI agents determined that an individual with the username "tinderbittles" registered an account on Playpen on February 3, 2015, and accessed the site for more than three hours between February 3 and March 4, 2015. (Residence Warrant

Aff. ¶¶ 25-26, Docket #39-1). This user accessed several posts that contained links to and sample photos of child pornography. (Residence Warrant Aff. ¶¶ 27-31). Agents learned the user's IP address via the NIT, determined the service provider of the IP address, and linked the IP address to Mr. Owens at his home in Kenosha, Wisconsin. (Residence Warrant Aff. ¶¶ 25-34).

1.2 The Residential Warrant

With this information, an FBI agent subsequently applied for a warrant to search the Kenosha residence. In support of the warrant application, the agent submitted a thirty-four-page affidavit that set forth his basis for probable cause to believe that the residence contained evidence relating to federal violations concerning child pornography. (*See generally* Residence Warrant Aff., Docket #39-1 at 8-41). This affidavit recited much of the information contained in the NIT Warrant Affidavit. (*See* Residence Warrant Aff. ¶¶ 7-21. United States Magistrate Judge Nancy Joseph signed the warrant on February 1, 2016. (Residence Warrant at 1).

Law enforcement officers executed the warrant on February 4, 2016, and seized—among other things—an external hard drive that contained numerous images and videos of suspected child pornography. (Criminal Complaint ¶ 5, Docket #1). Mr. Owens agreed to speak with law enforcement, and he admitted to accessing certain websites that contained images of child pornography. (Criminal Complaint ¶ 8). Based on the evidence seized from the residence and his statement to law enforcement, Mr. Owens was arrested pursuant to a criminal complaint that charged him with receiving and possessing child pornography. (*See* Criminal Complaint).

On March 1, 2016, a grand jury indicted Mr. Owens for one count of knowingly receiving child pornography, in violation of 18 U.S.C. §

2252A(a)(2), and one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5). (Indictment, Docket #9).

2. LEGAL STANDARD

Pursuant to 28 U.S.C. § 636(b)(1)(B), a magistrate judge may consider potentially dispositive motions, such as a motion to dismiss, and issue proposed recommendations to the district judge regarding the motion. When reviewing a magistrate's recommendation, the Court is obliged to analyze the portions of the report to which the defendant has lodged objections *de novo*. 28 U.S.C. § 636(b)(1)(C). Thus, the Court can "accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate." *Id.* In other words, the Court's *de novo* review of Magistrate Jones's Report is not limited to his legal analysis alone; rather, the Court may also review the factual findings and accept, reject, or modify those findings as it sees fit based upon the evidence. *Id.*

3. DISCUSSION

Mr. Owens raises the following arguments in support of his motion to suppress regarding the NIT Warrant: (1) the warrant was not supported by probable cause; (2) the warrant contained intentional or reckless misleading information; (3) the warrant was unconstitutionally broad and lacked particularity; (4) the triggering event for the anticipatory warrant never occurred; and (5) deployment of the NIT on Mr. Owens's computer exceeded the scope of the warrant. Mr. Owens further argues that the good faith exception does not apply to the flawed NIT warrant and thus, all evidence derived from NIT Warrant must be suppressed.

The Report rejects all Mr. Owens arguments and, as such, did not reach the question of whether the good faith exception would apply. As discussed below, the Court agrees with Magistrate Jones that the NIT Warrant was valid, and that suppression evidence is not warranted in this instance.

3.1 Probable Cause for the NIT Warrant

Mr. Owens argues that the Report erred in concluding that probable cause existed to issue the NIT Warrant. A search warrant may be issued only if it appears from the complaint or affidavit filed in support of it that there is probable cause to believe that an offense has been committed and that the defendant has committed it. *See* U.S. Const. amend. IV; Fed. R. Crim. P. 4(a). An affidavit has made a proper showing of probable cause when it sets forth facts sufficient to induce a reasonably prudent person to believe that a search thereof will uncover evidence of a crime. *Berger v. New York*, 388 U.S. 41, 55 (1967). In deciding whether a search warrant is supported by probable cause, courts must use the flexible totality-of-the-circumstances standard set forth in *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "Those circumstances need only indicate a reasonable probability that evidence of crime will be found in a particular location; neither an absolute certainty nor even a preponderance of the evidence is necessary." *United States v. Aljabari,* 626 F.3d 940, 944 (7th Cir. 2010) (citing *Gates,* 462 U.S. at 235). An issuing judge's "determination of probable cause should be paid great deference by reviewing courts," *Gates*, 462 U.S. at 236 (internal citation omitted).

Mr. Owens argues the NIT Warrant lacked probable cause because it failed to distinguish between people who accidently logged onto the Playpen site and people who actively sought child pornography. He argues this case

is distinguishable from *United States v. Gourde,* 440 F.3d 1065, 1070 (9th Cir. 2006), a Ninth Circuit case finding probable cause for a warrant to search the computer of someone based on their membership in a site that distributed child pornography.

Here, the Court agrees with the Report that the NIT Warrant was sufficiently supported by probable cause. Although Mr. Owens makes persuasive arguments in his objections to the Report, he fails to overcome the steep uphill battle that a defendant faces when challenging the existence of probable cause for a search warrant. The Court does not ask whether it would have found probable cause based on the same facts; instead, the Court is obliged to give "great deference" to the judge who issued the warrant. *Gates*, 462 U.S. at 236. Morever, the affidavit needed only show a reasonable probability that evidence of a crime will be found in a particular place. Under this standard, the Court simply cannot find that the NIT Warrant here lacked probable cause.

As the Report summarized, the NIT Warrant established the following facts regarding Playpen and its registered users: (1) the site operated only on an anonymous network that required users to download specific software before even finding the site; (2) finding the site required multiple, intentional steps; (3) users were unlikely to find the site without knowing its purpose and content; (4) the main page of the site depicted images that suggested the site contained child pornography and text that implied the site contained illicit images and/or videos; (5) users needed to register an account before they could access the site's content and were encouraged to use a fake email address when registering; (6) images and videos containing child pornography were available to all users who registered an account; and (7)

the majority of forums on the site were unambiguously dedicated to child pornography (example forum topics included "Jailbait – Boy," "Jailbait – Girl," "Preteen Videos – Girls HC," and "Toddlers"). (Docket #62 at 12).

Based on the totality of the circumstances, and when specifically taking into account the "great deference" to the magistrate's finding of probable cause, the Court is obliged to agree with the Report in finding that probable cause existed to issue the NIT Warrant. No single piece of information on its own provides a reasonable probability that evidence of a crime would be found, however, the Court finds that, when taken together, the affidavit as a whole provided a reasonable probability that evidence of a crime would be found on computers entering the Playpen website.

The Court fully recognizes, and agrees with Mr. Owens, that the case for probable cause here is nowhere near as strong as in the *Gourde* case where the intent to view child pornography was undoubtably clear. However, undoubtably clear is *not* the standard required for probable cause; the low level of certainty required for probable cause—less than a preponderance of the evidence—allows room for a much less certain case. Accordingly, the Court agrees with the Report that the issuing magistrate had a substantial basis for concluding that probable cause existed to issue the NIT Warrant. The motion to suppress will be denied on this ground.

3.2 *Franks* Hearing

Mr. Owens next argues that the Court should hold a *Franks* hearing because the NIT affidavit contains, at a minimum, misleading statements and omissions. (Docket #65 at 22) (citing *Franks v. Delaware*, 438 U.S. 154, 156 (1978). Specifically, Mr. Owens points to statements describing: (1) the

website's home page; (2) how the website could be found; (3) other miscellaneous information.

3.2.1 Legal Standard

In order for the Court to hold a *Franks* hearing to explore the validity of a search warrant affidavit, a defendant "must make a 'substantial preliminary showing' that: (1) the affidavit contained a material false statement; (2) the affiant made the false statement intentionally, or with reckless disregard for the truth; and (3) the false statement was necessary to support the finding of probable cause." *United States v. Maro,* 272 F.3d 817, 821 (7th Cir. 2001) (quoting *Franks,* 438 U.S. at 155-56).

"Franks makes it clear that affidavits supporting a search warrant are presumed valid, and that the 'substantial preliminary showing' that must be made to entitle the defendant to an evidentiary hearing must focus on the state of mind of the warrant affiant"—that is, the law enforcement officer who sought the search warrant. *United States v. Jones*, 208 F.3d 603, 607 (7th Cir. 2000) (citing Franks, 438 U.S. at 171). The inquiry is "not whether the affidavit contains a false statement, but whether the affiant knew or should have known that a statement was false." *United States v. Schultz*, 586 F.3d 526, 531 (7th Cir. 2009) (citing *Jones*, 208 F.3d at 603). The doctrine applies to omissions of fact in addition to false statement. *See United States v. Glover*, 755 F.3d 811, 817 (7th Cir. 2014).

The Seventh Circuit has noted that "[t]hese elements are hard to prove, and thus Franks hearings are rarely held." *United States v. Swanson*, 210 F.3d 788, 790 (7th Cir. 2000). Moreover, "an unimportant allegation, even if viewed as intentionally misleading, does not trigger the need for a *Franks* hearing." *Id.* at 791.

Ordinarily, an omission from a warrant affidavit is considered "material" if the court would not have authorized the warrant had it known the omitted facts. *Shell v. United States*, 448 F.3d 951, 954 (7th Cir. 2006); *Molina ex rel. Molina v. Cooper*, 325 F.3d 963, 970 (7th Cir. 2003) ("In order for a party to establish a *Franks* violation, there must be a reasonable probability that a different outcome would have resulted had omitted information been included in the affidavit"); *United States v. Pace*, 898 F.2d 1218, 1232-33 (7th Cir. 1990) (stating that an omission is material when "if the fact were included, the affidavit would not support a finding of probable cause"). The Court now turns to analyze the affidavit's purportedly misleading/false statements.

3.2.2 Statements Regarding Playpen's Home Page

Mr. Owens maintains that the government knowingly included in the warrant affidavit an incorrect description of Playpen's home page. (Docket #65 at 25). First, he points to the government's description of the picture on the main page. The affidavit indicates that, "[o]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." NIT Warrant Aff. ¶ 12. However, Mr. Owens maintains (and the government does not dispute) that at the time the warrant was signed, the website actually included "one small picture of a full-dressed young woman, sitting on a chair with her legs crossed." (Docket #65 at 25). Mr. Owens also point to the fact that the affidavit failed to mention how small the image was and that the most prominent feature of the homepage was its advertisement of its chat feature.

As to these statements, the Court agrees with the Report that they fail to meet the standard for a *Franks* hearing. Mr. Owens has not shown that the

inaccurate description of the homepage was made knowingly or with reckless disregard for the truth, or that it was material to the probable cause determination. In the Warrant Application, the affiant stated that he last accessed Playpen on February 18, 2015. (NIT Warrant Aff. ¶¶ 11-12). Between the last time he accessed the site and the time the warrant was authorized one day later on February 19, 2015, the homepage was apparently modified. There is no indication that the affiant knew about this change, purposefully provided misleading or false information in the Warrant Application, or intentionally excluded pertinent information from the Warrant Application. Based on these facts the Court finds it was not reckless for the affiant to submit a warrant application on February 19, based on how the website appeared on February 18. *See, e.g., Darby*, 2016 WL 3189703, at *9 ("There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015."); *Matish*, 2016 WL 3545776, at *12 ("The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant's authorization, as he had recently examined the website and confirmed that nothing had changed.").

As to the omissions regarding the image's size on the website or the prominent feature of the chat function, the Court finds Mr. Owens fails to show that their inclusion would have negated probable cause for the NIT Warrant. As discussed above, even if the affiant had accurately described the homepage, there would have been probable cause for the search. The Report describes the second image as that of a "young female wearing a short dress and fishnet stockings and posed in a sexually provocative manner would

suggest that the site contained, at the least, child erotica." (Docket #65 at 18). Thus, the actual appearance of the homepage was—regardless of the size of the image or chat function application—still suggestive of Playpen's pornographic content, and in any event, the appearance of the homepage was only one of several factors supporting the magistrate judge's determination of probable cause. As such, Mr. Owens fails to make a substantial showing that a *Franks* hearing is required based on the affidavit's description of the Playpen home page.

3.2.3 Location of Playpen

Mr. Owens also maintains that the affidavit misleadingly describes how difficult it is to find websites on the Tor network, "going so far as to suggest there is no such thing as a Tor equivalent of a Google search engine."(Docket #65 at 27). The affidavit indicated that it would be "extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content" because users had to take "numerous affirmative steps" just to find the site. (NIT Warrant Aff. ¶ 11). To support this conclusion, the affidavit explains that Playpen did not reside on the traditional Internet; a user therefore could access the site only through the Tor network and only if the user knew the site's web address. The affidavit suggests that a user could learn the web address while communicating about, or looking for, child pornography elsewhere on the Internet. The affidavit further explains that user could not find Playpen via a Google search and instead that Playpen was listed on a Tor hidden service page that was dedicated to pedophilia and child pornography.

Even assuming the government's statements about the ease of locating Playpen were misleading and/or reckless, the Court would still find that

information was not necessary to support the finding of probable cause. *See Darby*, 2016 WL 3189703, at *8 ("Ultimately, no matter how searchable the Tor network may be, the magistrate judge would have been justified in concluding that those individuals who registered and logged into Playpen had knowledge of its illegal content."). As the *Darby* court noted in its finding of probable cause for the NIT Warrant, the Tor network is, at the very least, less searchable than the regular Internet and is an "obvious refuge for those in search of illegal material." *Id.* The affidavit does not purport that *every* Playpen user necessarily intended to access child pornography, but instead only reaches the conclusion that it was "extremely unlikely" that a user would find Playpen without understanding its illegal purpose. (NIT Aff. ¶ 10). Based on these factors, the Court finds that without the affidavit's alleged misleading statements, the magistrate's common sense judgment still could have lead her to believe that an individual would only take the steps necessary to log onto Playpen in order to seek illegal child pornography. Thus, Mr. Owens fails to make a showing for a *Franks* hearing based on statements regarding the location of Playpen.

3.2.4 Miscellaneous Statements

Finally, Mr. Owens points to various other misleading statements and omissions, including: (1) the false statement that the "entirety" of Playpen was "dedicated to child pornography"; (2) omitting any details regarding which sub-forums on Playpen contained illegal pornography; and (3) suggesting that common features of the site were indicative of criminality. (Docket #65 at 29-30).

Like the Report, the Court does not find any of this information to rise to the level of a material statement or omission. The affidavit's assertion that

Playpen was "dedicated" to child pornography is not the same as suggesting no legal content existed on the website. As to the sub-forums, the affidavit describes those that contained "the most egregious examples of child pornography and/or dedicated to retellings of real world hands on sexual abuse"—and does not purport to describe all sub-forums of Playpen. (*See* NIT Aff. ¶ 27). Thus, none of the miscellaneous allegedly false or misleading statements meet the standard for a *Franks* hearing.

3.2.5 Summary

In sum, the Court finds that Mr. Owens has failed to make the requisite "substantial preliminary showing" to justify holding a *Franks* hearing in this case. Mr. Owens argues that the Report erred in not considering all the alleged false statements and/or omissions collectively when determining whether the information was necessary to support a finding of probable cause. (Docket #65 at 31). The Court, however, disagrees. The Report found that statements regarding the description of the Playpen Homepage did *not* qualify as reckless—failing prong two of the *Franks* test. Similarly, the Report found that miscellaneous statements about Playpen's dedication to child pornography did not qualify as material false or misleading statements—failing prong one of the *Franks* test. As such, the Report did not err in failing to consider all allegedly false statements and/or omissions in considering whether probable cause would have existed. In light of the foregoing, the Court is obliged to adopt the Report's recommendation and deny the request for a *Franks* hearing.

3.3 NIT WARRANT—Breadth and Particularity

Mr. Owens next argues that the NIT Warrant was invalid because it was overbroad and lacked particularity. (Docket #65 at 33). The Report

recommends denying the motion to suppress on these grounds. (Docket #62 at 13-15).

Mr. Owens argues that the NIT was overbroad because it could have, but failed to, exclude individuals who broke no laws. Instead of narrowing the warrant only to authorize searches of visitors who actually viewed or downloaded illegal child pornography, the "FBI sought the broadest possible search authorization, encompassing many thousands of targets who may have done and intended to do nothing illegal." (Docket #65).

The Court rejects this argument and finds that the NIT Warrant did not exceed the probable cause on which it was based. As discussed above, the NIT affidavit established a fair probability that *any* user who logged onto Playpen did so with intent to access child pornography. As several other courts have already held, the fact that the government *could* have and eventually did narrow its search, is immaterial. *See, e.g., Matish*, 2016 WL 3545776, at *14.

Next, as to the particularity argument, the Constitution demands that two things in a warrant be described with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006). The NIT warrant meets both requirements. Attachments A and B of the NIT warrant, respectively, identified the "Place to be Searched" and the "Information to be Seized." (NIT Warrant at 3-4). Attachment A describes the places to be searched as follows: "This warrant authorizes the use of a network investigative technique ('NIT') to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." (NIT Warrant at 3). In light of these specific descriptions, the Court finds that

a law enforcement executing the warrant would know "exactly what he was authorized to search (computers of users who logged into Playpen) and seize (the seven pieces of information described in Attachment B)." (Report, Docket #62 at 14). As such, the Court finds the NIT Warrant was sufficiently particular.

In light of the foregoing, the Court finds that the NIT Warrant was not unconstitutionally overbroad or lacking in particularity. The Court will therefore deny the motion to suppress on these grounds.

3.4 Triggering Event for NIT Warrant

Next, Mr. Owens argues that the NIT Warrant was an anticipatory warrant and the "triggering event" for the computer searches never occurred. (Docket #65 at 38). The Report recommends denying the motion to suppress on this ground. (Docket #62 at 23).

"An anticipatory warrant is 'a warrant based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of crime will be located at a specified place.'" *United States v. Grubbs*, 547 U.S. 90, 94 (2006) (quoting W. LaFave, Search and Seizure § 3.7(c), p. 398 (4th ed. 2004)). An anticipatory warrant has two prerequisites to be valid: (1) the "triggering event"; and (2) probable cause that the triggering event will occur. *Id.* at 96-97.

Here, the NIT Warrant authorized searches whenever a user signed onto Playpen, with the "triggering event" for the searches being the act of accessing the website, as described in the warrant. (*See* NIT Warrant ¶ 32). Mr. Owens argues that the triggering event never occurred in this instance because at the time the warrant was signed, the Playpen website looked different from the warrant description (again focusing the image change on

the website as described above). Since the warrant application incorrectly described Playpen's home page logo, Mr Owens argues he could not log into Playpen via the home page described in the warrant application because that home page no longer existed. Thus, Mr. Owens argues, the search conducted in this case was not authorized by the NIT Warrant.

The Court agrees with the Report in finding that the triggering event of the anticipatory NIT Warrant was logging into Playpen while it was under government control. As such, the triggering event was not conditional upon the website's home page logo but upon whether a user or administrator of Playpen logged into the site, which the warrant identified by its specific URL. The Court notes this finding is consistent with the majority of courts who have addressed this precise issue. *See, e.g., Anzalone*, 2016 WL 5339723, at *8; *Matish*, 2016 WL 3545776, at *15; *Darby*, 2016 WL 3189703, at *9; *Eure*, 2016 WL 4059663, at *7. As such, the Court will deny the motion to suppress on this ground.

3.5 NIT Deployment on Wisconsin Computer

Finally, Mr. Owens argues that the search of his computer in Kenosha, Wisconsin, exceeded the scope of the NIT Warrant's authorization because the warrant authorized *only* searches in the Eastern District of Virginia. (Docket #65 at 39-42). The Report recommended denying the motion to suppress on this ground, and the Court agrees with the Report.

The Court finds that Mr. Owens's argument requires an overly narrow reading of the NIT Warrant that ignores the sum total of its content. *See United States v. Michaud*, Case No. 15-CR-05351, 2016 WL 337263 at *3-*4 (W.D. Wash. Jan. 28, 2016).While the NIT Warrant cover sheet does explicitly

reference the Eastern District of Virginia, that reference must be viewed within context:

> An application by a federal law enforcement officer...requests the search of the following person of property located in the Eastern District of Virginia (identify the person or describe the property to be searched and give its location):
> See Attachment A[.]

(NIT Warrant at 2, Docket #39-2).

The warrant explicitly invites the magistrate judge to "give its location" in the blank space provided, wherein the phrase, "See Attachment A," is inserted. Attachment A, subtitled "Place to be Searched," authorizes deployment of the NIT to "all activating computers," defined as "those of any user or administrator who logs into [Playpen] by entering a username and password." (NIT Warrant at 3). Attachment A refers to the Eastern District of Virginia as the location of the government-controlled computer server from which the NIT is deployed. (NIT Warrant at 3). As such, a reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia. Accordingly, the Court finds that search of Mr. Owens's computer in Wisconsin did not exceed the scope of the NIT Warrant, and the Court will deny the motion to suppress on this ground.

4. CONCLUSION

In sum, the Court agrees with Magistrate Jones and the majority of other courts in finding that suppression of the evidence is not warranted in

this case based on any of Mr. Owens's arguments presented here. Thus, the Court will adopt the Report in full and deny Mr. Owens's motion to suppress the evidence.

Accordingly,

IT IS ORDERED that Magistrate Judge David E. Jones's report and recommendation (Docket #62) be and the same is hereby **ADOPTED**;

IT IS FURTHER ORDERED that, consistent with the Court's adoption of the report and recommendation, Mr. Owens's motion to suppress (Docket #37) be and the same is hereby **DENIED**.

Dated at Milwaukee, Wisconsin, this 5th day of December, 2016.

BY THE COURT:

s/ *J. P. Stadtmueller*
J.P. Stadtmueller
U.S. District Judge